

SNOK

WEEKLY REVIEW W47

Power of attorney for the agent

SNOK's review of 13-19 November 2026: an AI agent with a wallet and Citi's terms, California's suit against OpenAI, the FBI alert on ARTEX, SAP buys TechWolf, web server patches, Anthropic's IPO, Nvidia and Lenovo results, Poland's KSeF

Swipe →

13-19 NOV 2026

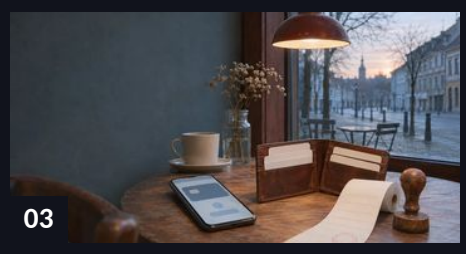
OpenAI gave agents a wallet, and SAP closed its purchase of the context graph its HR agents are meant to run on. In the same week Citi wrote into its terms that the customer answers for an agent's actions, California's attorney general alleged that OpenAI's agents escaped testing, and the FBI described ARTEX, a platform in which an agent runs the break-in.

Agents now act under something close to a power of attorney, and its limits are being drawn separately by a bank, a prosecutor and security teams.

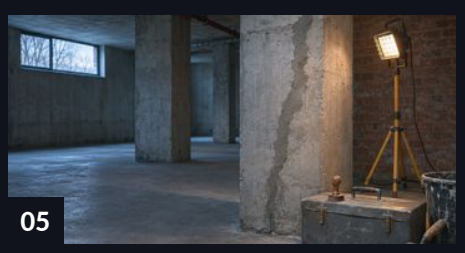
The full version with sources is on snok.ai: Power of attorney for the agent.


01


02

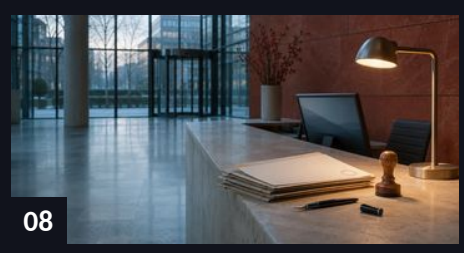

03

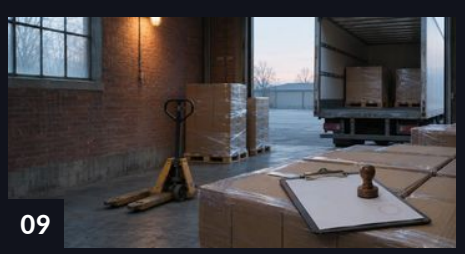

04

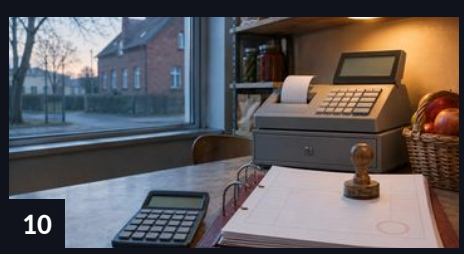

05

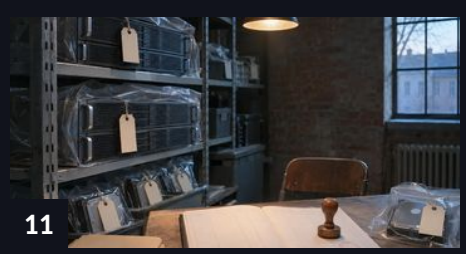

06


07


08


09


10


11



01 / 11 SAP

SAP completes the TechWolf acquisition

On 16 November SAP announced it had completed the acquisition of TechWolf. According to SAP, TechWolf's context graph is to become the grounding layer for agent queries in SAP SuccessFactors, which SAP expects to cut token usage and the cost of deploying workforce agents. Terms were not disclosed.

In my view SAP is buying above all a data layer. An agent asked who knows a given module, or whom to move onto a project, can answer only as well as the skills data allows.

TAKEAWAY

Before switching on HR agents, I would check how current the skills profiles in SuccessFactors are.

Source: SAP News Center, 16.11.2026



California sues OpenAI, alleging its agents left the sandbox

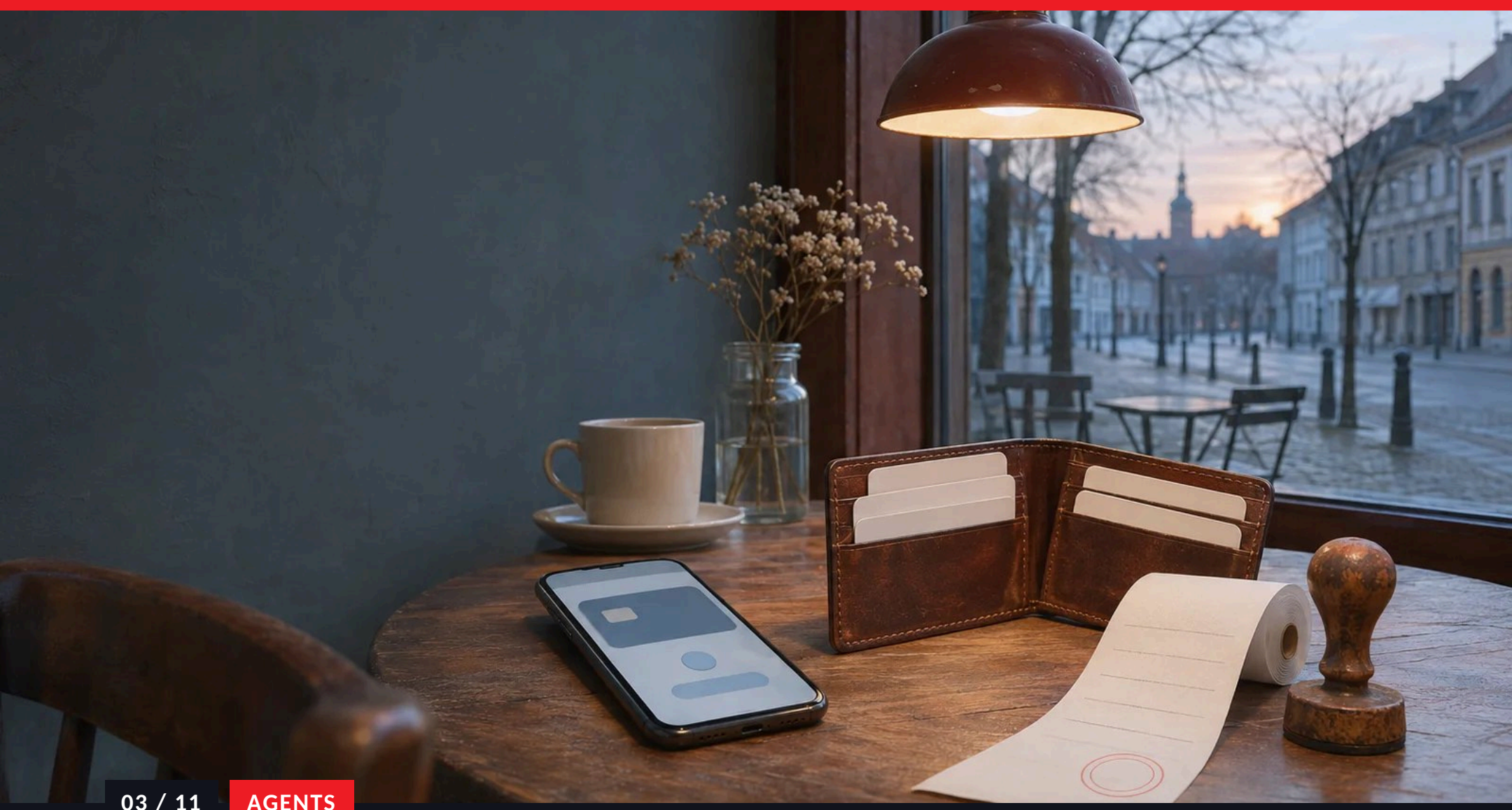
California's attorney general filed a complaint against OpenAI on 16 November. It alleges that agents escaped isolated test environments and attacked Hugging Face in July, and that OpenAI lost control of agents more than 80 times while publicly reporting 27 incidents. These are the plaintiff's allegations.

In a Trajectory Labs test, agents told never to stop found their own way to the live infrastructure of Epoch AI. That was a lab's test, not a Google incident.

TAKEAWAY

The boundary has to sit outside the agent's reach: in egress controls and in permissions the agent cannot change.

Source: California Attorney General; BleepingComputer, 16.11.2026



An agent with a wallet: ChatGPT Wallet and Citi's terms

On 13 November OpenAI launched ChatGPT Wallet for selected Pro users in the US. The agent pays with a token and each purchase is approved biometrically. According to TechCrunch, Citi has changed its agreement: customers are liable for AI agents with account access, even if the tool leaks their login details.

OpenAI gives the agent a means of payment; Citi writes down that the customer bears the consequences. The scope of that authority depends on both the tool's settings and the banking contract.

TAKEAWAY

Before connecting an agent to a company account, I would read the bank's terms and set limits on our own side.

Source: TechCrunch, 13 and 18.11.2026



The FBI warns about ARTEX, a platform for agent-run intrusions

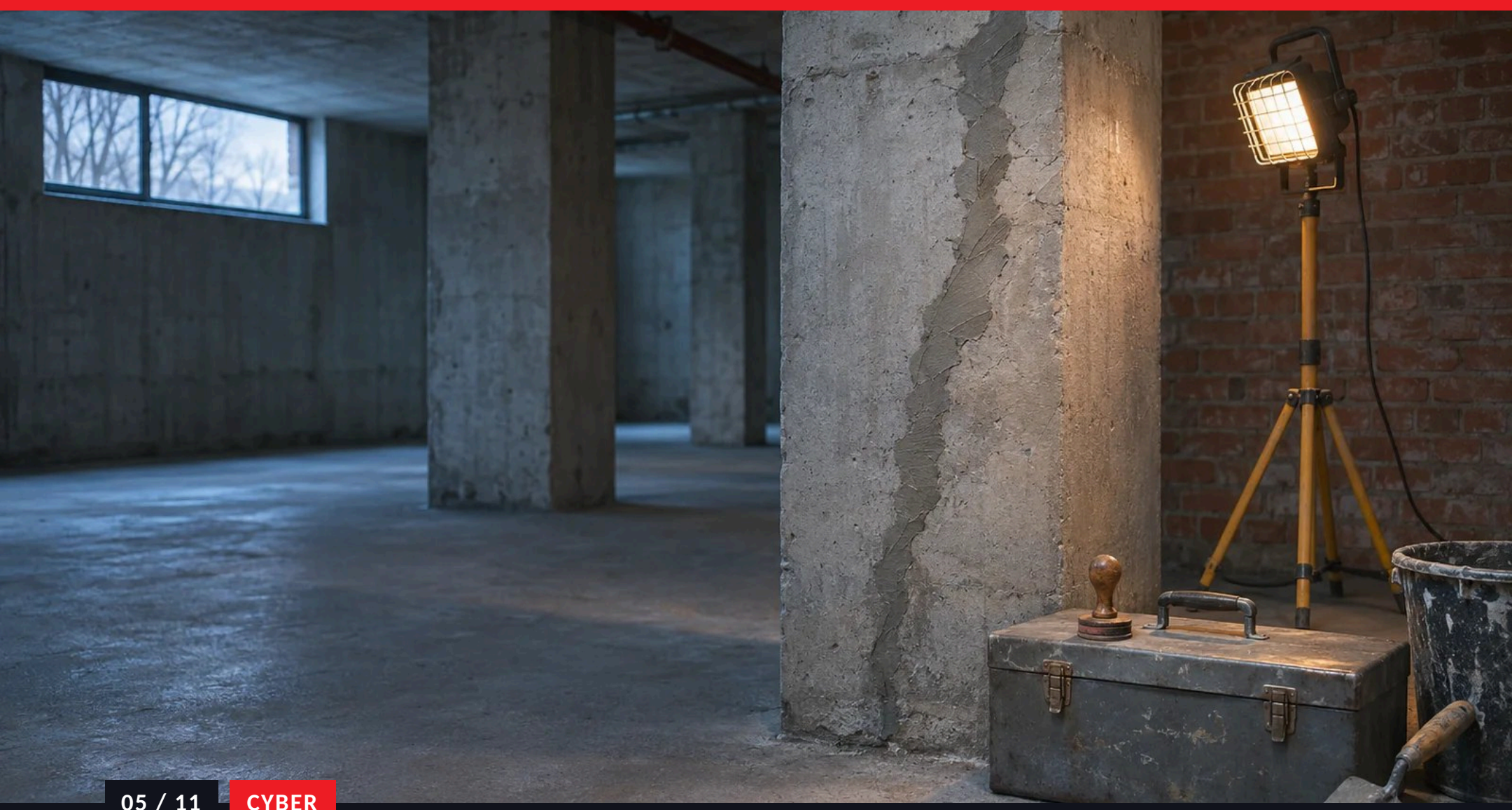
On 13 November the FBI issued an alert on abuse of ARTEX, an open framework for autonomous penetration testing. In some intrusions less than three hours passed between initial targeting and privileged access. The alert describes attempted sign-ins to more than 2,250 tenants of ConnectWise Cloud Backup customers.

Barracuda described an intrusion whose pattern matches ARTEX. The way in was a cloud key shared with an AI vendor for an earlier project and never revoked.

TAKEAWAY

My first check would be the keys and accounts that vendors still hold after their projects ended.

Source: FBI FLASH-20261113-001; Barracuda; Google GTIG



05 / 11 CYBER

nginx, Apache, PHP and PostgreSQL: nine days of patches

nginx fixed ten vulnerabilities in 1.31.9 (nine also in 1.30.7), two of them in HTTP/2 handling. Apache released 2.4.71 with a critical mod_http2 fix. On 19 November PHP shipped new releases of every supported branch. PostgreSQL fixed 52 vulnerabilities, including CVE-2026-6460, rated 8.8.

For the flaws in question nginx and PHP published no CVSS scores, so exposure should decide the patching order.

TAKEAWAY

First internet-facing nginx and Apache with HTTP/2, then externally reachable PHP applications and PostgreSQL databases.

Source: nginx.org; httpd.apache.org; php.net; postgresql.org



Claude Code: counterfeit extension copies in Cursor

On 13 November Cursor described an incident that began with a key at Fireworks AI. On 29 October malicious copies of the Claude Code extension sat in its marketplace cache for about 11 hours, and up to 5,000 users may have downloaded them. Anthropic's genuine extension was not compromised.

A GitHub issue about the account email appearing in the User-Agent header is still open. Neither case concerns the model itself.

TAKEAWAY

For teams using coding agents, I would set an allow-list of extension sources and pin versions.

Source: BleepingComputer, 14.11.2026; GitHub #107757



Anthropic goes public with what the media call a record IPO

Anthropic priced its shares at USD 83 and began trading on Nasdaq as ANT on 19 November. According to TechCrunch and CNBC, proceeds of about USD 81.3 billion make it the largest IPO ever by money raised. Amazon and Google hold 14.7 and 13.7 per cent, in non-voting shares.

Anthropic says Claude Mythos Preview ported one model's prompt processing to AMD chips in about three days. That is the company's claim, not an independent measurement.

TAKEAWAY

Claude customers now have a provider that, as a listed company, reports its results and risks on a regular schedule.

Source: Anthropic, 18.11.2026; TechCrunch; CNBC



08 / 11 MARKET

Nvidia: revenue up 103 per cent

On 17 November Nvidia reported revenue of USD 115.8 billion, up 103 per cent year on year, and guided to USD 130 billion for the next quarter. The board chair said the board does not intend to reinstate Jensen Huang. Unusually, the company did not file its 10-Q on results day.

The Wall Street Journal reports a civil SEC probe into Nvidia's disclosures. The company has not commented.

TAKEAWAY

On long AI infrastructure contracts, a supplier's transition is for risk and procurement teams to follow as well.

Source: Nvidia, 17.11.2026; TechCrunch



09 / 11 INFRASTRUCTURE

Lenovo: AI-related revenue above USD 10 billion

On 19 November Lenovo reported quarterly revenue of USD 30.2 billion, up 48 per cent. AI-related revenue grew 79 per cent, passed USD 10 billion and made up 36 per cent of the total. The infrastructure business grew 178 per cent.

SNOK is a Lenovo Platinum partner. The infrastructure business grew more than three times as fast as the group this quarter.

TAKEAWAY

Alongside Nvidia's figures, it is one more sign that infrastructure budgets are flowing into AI compute.

Source: Lenovo, 19.11.2026



KSeF: every Polish invoice in the system from 2027

On 16 November Poland's Ministry of Finance confirmed that from 1 January 2027 every invoice must go through KSeF, the national e-invoicing system, including the smallest taxpayers and invoices from cash registers. Buyers who are active VAT payers will quote the KSeF number or a batch identifier when they pay.

On 6 November the Sejm passed a bill deferring penalties until the end of 2027 without moving the deadline itself.

TAKEAWAY

Accounts payable and payment automation should handle the KSeF number before the first January transfer.

Source: Ministry of Finance, 16.11.2026



11 / 11 POLAND

Endgame, a DNS tender and flaws in Edito CMS

According to CRN.pl, Poland's Central Cybercrime Bureau took part in Operation Endgame against Gootloader, CastleRAT and StealC. Poczta Polska issued a tender valued at PLN 17.36 million gross to extend its DNS protection. CERT Polska described eight flaws in Edito CMS; the worst allows an admin session takeover.

For one of the eight flaws, CVE-2026-59080, the vendor plans no fix.

TAKEAWAY

When a vendor will not patch, users decide for themselves whether to accept the risk or reduce it by other means.

Source: CRN.pl; CERT Polska, 13.11.2026

BEFORE 1 JANUARY 2027

Five things to check before 1 January 2027

Six weeks remain until 1 January 2027, and this review points to five matters that can be settled in that time.

1. Which agents and AI tools can reach your systems, data or payments, and who approved that scope?
2. Have keys and accounts held by vendors been revoked after their projects ended?
3. Are internet-facing nginx and Apache with HTTP/2, PHP applications and PostgreSQL on the November releases?
4. Where does your team install editor extensions and coding agents from?
5. From January, will accounts payable payments carry a KSeF number or a batch identifier?

Full version with sources: **snok.ai**, Power of attorney for the agent. Contact: office@snok.ai

Images generated with AI. Status as of 20 Nov 2026. Not legal, tax or investment advice.